

UNITED STATES DISTRICT COURT

for the

____ District of _____

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

)))))))

Case No.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section**Offense Description*

The application is based on these facts:

- Continued on the attached sheet.
- Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Printed name and title

Sworn to before me and signed in my presence.

Date: _____

Judge's signature

City and state: _____

Printed name and title

ATTACHMENT A-1**PROPERTY TO BE SEARCHED**

10201 Lindley Avenue, Apartment H117, Northridge, CA 91325 (the "SUBJECT PREMISES"), including any digital devices contained therein. The SUBJECT PREMISES is located within a multi-building apartment complex named "Grand Apartments on Lindley." The apartment complex has a leasing office on Lindley Avenue with the marking "10201" on the top front of the office entrance. The SUBJECT PREMISES is located within Building "H", in the northwest area of the apartment complex. Building H is a three-story, brown and white in color building. There is a parking garage with numbered parking spaces beneath Building H. There are two floors of apartments at Building H. The SUBJECT PREMISES is located on the first floor of apartments at Building H. A set of concrete stairs leading to a black metal security door, which is located within a publicly accessible parking lot area on Lindley Avenue, allows access into a courtyard area where Building H is located. The SUBJECT PREMISES is approximately 50 yards from the metal security door. There are sidewalks in the courtyard area that provide pedestrian access to multiple residences, including the SUBJECT PREMISES. There is a green in color, metal-type construction dog waste container approximately 10 to 15 feet in front of the SUBJECT PREMISES. The SUBJECT PREMISES has a teal in color door with a white door frame. The door opens inward and has a silver door knob and a silver deadbolt located on the right side of the door. There is a bronze door knocker in the center of the door. There is a

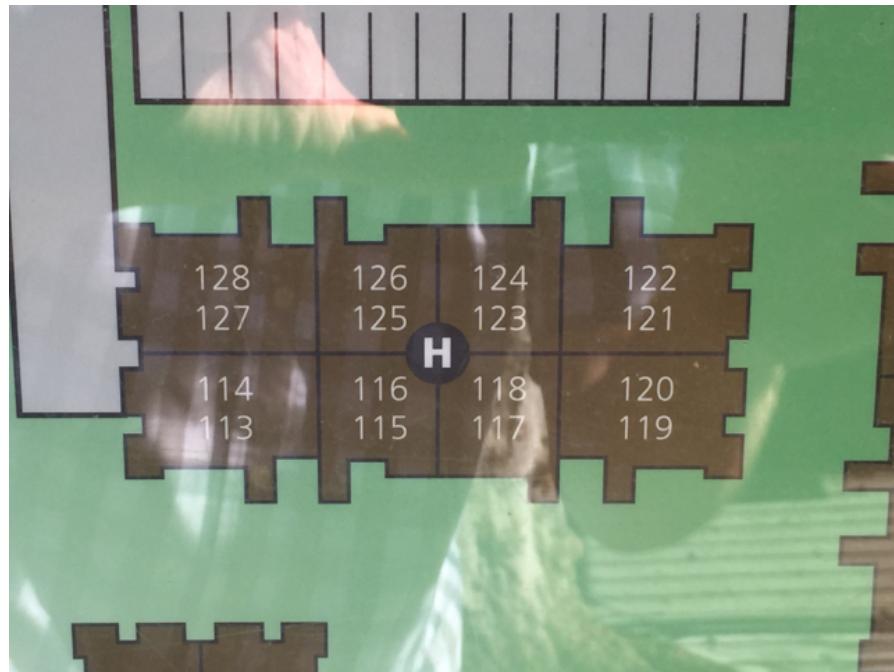
small sign showing "H117" affixed to a wall and located to the left side of the door.



Photograph of the Leasing Office depicting the street number.



Photo of directory showing leasing office (bottom center) and subject residence on top right with red arrow.



Close-up photo of directory showing location of apartment H117.



Photo of front entrance to apartment H117.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are contraband, evidence, fruits, and instrumentalities of violations of 21 U.S.C. § 843(a)(3) (acquiring or obtaining a controlled substance by misrepresentation, fraud, deception, or subterfuge); 21 U.S.C. 841(a)(1) (distribution and possession with intent to distribute controlled substances); 18 U.S.C. § 641 (theft of government property); 18 U.S.C. § 1001 (false statements); and 18 U.S.C. § 1035 (false statements related to healthcare matters) (the "SUBJECT OFFENSES") namely:

- a. Any controlled substances and their containers;
- b. Currency, money orders, bank checks, or similar monetary instruments in quantities over \$1,000;
- c. Property of the Department of Veterans Affairs;
- d. Any and all documents created by, or from, or concerning recordkeeping machines or programs of the United States or the Department of Veterans Affairs concerning the storage, monitoring, distribution, or other tracking of controlled substances;
- e. Any evidence of use of controlled substances diverted from the Department of Veterans Affairs or of the same type as those diverted from the Department of Veterans Affairs, such as track marks or drug paraphernalia.
- f. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers

dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

g. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

h. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

i. Records, documents, programs, applications, materials, or conversations relating to the trafficking of drugs, including ledgers, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed;

j. Audio recordings, pictures, video recordings, or still captured images relating to the possession or distribution drugs and the collection or transfer of the proceeds of the above-described offenses;

k. Contents of any calendar or date book;

1. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

m. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

n. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output

devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICE

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine

whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized,

the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. During the execution of this search warrant, with respect to any biometric sensor-enabled device that falls within the scope of the warrant, law enforcement personnel are authorized to: (1) depress the CARIAGAKAMEI's thumb- and/or fingerprints onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of CARIAGAKAMEI's face with her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Christ Kong, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is submitted in support of an application for a warrant to search:

a. A residence located at 10201 Lindley Avenue, Apartment H117, Northridge, CA 91325 (the "SUBJECT PREMISES"), as further described in Attachment A-1;

b. A copy of the California Department of Justice, Bureau of Criminal Identification and Investigative Services, Prescription Drug Monitoring Program/Controlled Substance Utilization Review and Evaluation System ("CURES") Program for prescription records for the past three years for CILEISHALYN CARIAGAKAMEI ("CARIAGAKAMEI"), as further described in Attachment A-2;

c. A 2017 White Dodge Challenger bearing California License Plate number 8BMR346 and Vehicle Identification Number (VIN) 2C3CDZBT2HH636590, (the "SUBJECT VEHICLE") as further described in Attachment A-3;

d. CARIAGAKAMEI's employee locker, #24, (the "SUBJECT LOCKER") located within the West Los Angeles ("WLA") VA Medical Center ("VAMC"), a medical facility within the Greater Los Angeles Healthcare System ("VAGLAHS") of the Department of Veterans Affairs ("VA"), as further described in Attachment A-4;

e. CARIAGAKAMEI's person, including for items on her and for a visual inspection of her hands, arms, and feet, as described in Attachment A-5.

2. The requested search warrant seeks authorization to seize evidence, fruits, and instrumentalities of violations of 21 U.S.C. § 843(a)(3) (acquiring or obtaining a controlled substance by misrepresentation, fraud, deception, or subterfuge); 21 U.S.C. 841(a)(1) (distribution and possession with intent to distribute controlled substances); 18 U.S.C. § 641 (theft of government property); 18 U.S.C. § 1001 (false statements); and 18 U.S.C. § 1035 (false statements related to healthcare matters) (the "SUBJECT OFFENSES") as further described in Attachment B.

3. Attachments A-1 through A-5 and B are incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related only in substance and in part.

II. BACKGROUND FOR SPECIAL AGENT CHRIST KONG

5. Since April 2018, I have been a Special Agent ("SA") with the VA Office of Inspector General ("VA-OIG"), Criminal

Investigations Division. My primary duties are to conduct investigations of violations of federal criminal laws. I have completed specialized law enforcement training courses at the Federal Law Enforcement Training Center involving drug investigations. I also completed various federal training courses covering various topics like drug use, drug distribution, and drug diversion against the government.

6. Prior to my employment with the VA-OIG, I was a Criminal Investigator with the Air Force Office of Special Investigations ("AFOSI") - Office of Procurement Fraud, where I investigated felony-level crimes, from August 24, 2014 to April 28, 2018. Prior to my employment with the AFOSI, I was a Correctional Officer with the Federal Bureau of Prisons, where I assisted with criminal investigations occurring within the United States prison system, from April 7, 2013 to February 24, 2014.

7. I have participated in numerous investigations into violations of federal law, including investigations into the illegal possession and distribution of controlled substances, as well as false and fraudulent statements against, and thefts of the property of, the United States. I have also spoken to more experienced colleagues about their experiences concerning such investigations.

8. Based on my training, experience, and discussions with more experienced colleagues, I am familiar with the methods used to divert drugs from the United States and the VA, as well as the methods typically used to attempt to conceal such diversion.

III. SUMMARY OF PROBABLE CAUSE

9. On or about June 11, 2018, T.W., a veteran and patient of the WLA VAMC, contacted the VA to report that CARIAGAKAMEI, a Registered Nurse ("RN") at the WLA VAMC, had been diverting narcotics from the WLA VAMC and her patients in order to offer them to T.W. and to retain them for her personal possession or use. In connection with these allegations, T.W. provided the VA with pictures of narcotics vials bearing unique VA lot numbers, which vials T.W. reported photographing at the SUBJECT PREMISES.

10. T.W. reported that he and CARIAGAKAMEI had been involved in an approximately five-month romantic relationship, which began after they met as patient and nurse, and that T.W. lived with CARIAGAKAMEI, in the SUBJECT PREMISES, from on or about December 26, 2017 to a day in or around the first week of June, 2018. T.W. described CARIAGAKAMEI as owning a White Dodge, consistent with the SUBJECT VEHICLE, which is registered to CARIAGAKAMEI.

11. In light of T.W.'s allegations, VA colleagues investigated records from a comprehensive, automated medication management machine commonly referred to as Omnicell ("Omnicell"), through which VAMC doses of controlled substances are dispensed and monitored. Omnicell records for CARIAGAKAMEI's Hydromorphone HCL (a narcotic drug and controlled substance commonly known as "Dilaudid") dosing and data entry over a four-day period from May 31, 2018 through June 3, 2018 reflect anomalies and discrepancies that a VAMC clinical pharmacist has described as "highly unusual and very

suspicious." The clinical pharmacist emphasized that (s)he has "never observed any activity" as "egregious" as that suggested by CARIAGAKAMEI's Omnicell dose distribution and dose logging activity.

IV. STATEMENT OF PROBABLE CAUSE

12. Based on my review of law enforcement reports, my conversations with law enforcement officers and clinical staff members of the VAMC, my own observations and knowledge of the investigation, and my training and experience, I am aware of the following:

A. T.W.'s ALLEGATIONS CONCERNING CARIAGAKAMEI

13. VA employment records show that CARIAGAKAMEI began as an RN at the WLA VAMC on or about July 9, 2017. From my discussions with other investigators, I am aware that CARIAGAKAMEI has an active California Registered Nurse License under License Number 95073176, and that a search of criminal databases establishes that she has no criminal record.

14. On or about June 11, 2018, T.W., a veteran, disclosed to a VA employee that CARIAGAKAMEI was diverting VA controlled substances. T.W. emailed a WLA VAMC Assistant Nurse Manager, E.J., on June 11, 2018 at 4:13PM. The subject of the email was, "CileishaLyn CariagaKamei stolen Morphine and other controlled substances" [sic]. T.W. stated in the email that he was providing photographs evidencing that CARIAGAKAMEI had illegally diverted and possessed controlled substances at the SUBJECT PREMISES. T.W. said he was reporting CARIAGAKAMEI because he believed she would "exploit other people in similar situations."

15. On or about June 11, 2018, at 2:00PM, T.W. called another supervising RN at the VAMC, M.D., and alleged that CARIAGAKAMEI was giving T.W. "IV morphine" that CARIAGAKAMEI had stolen from patients. TW provided his phone number and asked M.D. to call him back.

16. M.D. met with E.J. on the same day, at approximately 2:30PM, and told E.J. about T.W.'s phone call. E.J. then called T.W. at the phone number T.W. had provided, and T.W. told E.J. that T.W. had lived with CARIAGAKAMEI at CARIAGAKAMEI's apartment from approximately December 26, 2017 until the prior week (the first full week of June 2018).

17. T.W. alleged that CARIAGAKAMEI had given T.W. "IV morphine," because T.W. had pain, and that CARIAGAKAMEI took the medications from her "dying" patients. T.W. also said that CARIAGAKAMEI used marijuana and cocaine, and that T.W. feared CARIAGAKAMEI because CARIAGAKAMEI was "mean and abusive."

18. Over the following two days, I and my colleagues conducted interviews of VAMC employees who had communicated with T.W. concerning his allegations, as well as T.W. himself. From this, we learned the additional following facts:

a. T.W. was an inpatient at WLA VAMC from November 2017 to December 2017. T.W. said that CARIAGAKAMEI had given him extra medication while he was an inpatient at the WLA VAMC. T.W. was a patient on ward 3-South, knew CARIAGAKAMEI as "Leisha," and alleged that he and CARIAGAKAMEI had met and developed a relationship during that time.

b. During this period, T.W. had been prescribed Oxycodone, 1-2 morphine pills, and a wrist IV, because he was in a lot of pain. T.W. specifically recalled one occasion during this period where CARIAGAKAMEI dropped pain medication on the floor and said, "whoops, I'll get some more." I have spoken with other investigators, and they understood this report of CARIAGAKAMEI's actions and words as an effort by her to divert VAMC controlled substances to her personal possession.

c. By December 26, 2018, CARIAGAKAMEI asked T.W. to stay at the SUBJECT PREMISES so that CARIAGAKAMEI could take care of T.W. A few nights later, T.W. said, CARIAGAKAMEI gave T.W. "Hydromorphone" [sic], obtained from the VA, while they were at CARIAGAKAMEI's apartment.

d. Approximately three months ago, according to T.W., he and CARIAGAKAMEI decided to visit a methadone clinic outside of the VA to deal his issues.

e. T.W. said that his relationship with CARIAGAKAMEI became toxic when T.W. found out that CARIAGAKAMEI had more medication from the VA. As a result, T.W. confronted CARIAGAKAMEI about ending their relationship, and CARIAGAKAMEI said she obtained the medication from a deceased patient and that she planned to use the medication for her back pain, which prompted T.W. to take pictures of the medication. T.W. said he ultimately determined to end the relationship because of CARIAGAKAMEI's hard-partying, binge-drinking, suicidal thoughts, and erratic behavior.

f. T.W. said he was last inside of CARIAGAKAMEI's apartment on June 8, 2018, and observed a bottle of morphine in a three-drawer "plastic thing" in a bookshelf.

g. T.W. expressed fear of and concern for CARIAGAKAMEI. T.W. said that CARIAGAKAMEI used drugs, and that CARIAGAKAMEI told him that she used drugs. T.W. did not see CARIAGAKAMEI using drugs or see puncture marks on her body.

h. However, T.W. also said that CARIAGAKAMEI used Oxycodone, morphine extended release, and morphine 60 milligrams, and that she was not prescribed any medications when she took the drugs.

i. T.W. said he saw loose Oxycodone pills in the center console of CARIAGAKAMEI's vehicle, and T.W.'s description of the vehicle was consistent with the SUBJECT VEHICLE.

j. T.W. stated that CARIAGAKAMEI had a lot of hiding places for drugs at her apartment. T.W. said CARIAGAKAMEI took medications throughout the day; he saw medications in individual "blister packs," and he knew CARIAGAKAMEI took pills, which she stored in a tan fabric square container in the kitchen, adjacent to the dishwasher and an upper cabinet, at her apartment. T.W. said the pills were in the top right drawer, where other medication was located. T.W. believed CARIAGAKAMEI saved medications because she had an upcoming surgery or procedure. T.W. added that CARIAGAKAMEI mentioned usage of cocaine, but T.W. had not seen her use it.

k. T.W. said that CARIAGAKAMEI had been suicidal for the past few weeks, and that CARIAGAKAMEI took drugs from patients who were dying.

19. From my review of T.W.'s criminal record, I am aware of the following:

a. On or about June 2, 2010, T.W. was arrested in Florida by the Miami Police Department for Felony Larceny. On February 8, 2011, the court deferred the matter through pretrial diversion.

b. On or about December 15, 2012, the Riverside County Sheriff's Department arrested T.W. for First Degree Robbery. T.W. was convicted of misdemeanor battery, misdemeanor petty theft, and felony possession of a controlled substance. T.W. received a sentence of 90 days in jail, 36 months of probation and was fined. On July 5, 2013, T.W. was then sentenced to 101 days in jail for a probation violation. On May 20, 2015, the conviction was set aside and dismissed.

c. On December 30, 2012, T.W. was arrested by the Riverside County Sheriff's Department for possession of narcotic controlled substance, possession of controlled substance, and possession of unlawful paraphernalia. The possession of narcotic controlled substances proceedings were suspended and diversion term was successful, which resulted in dismissal.

d. On May 21, 2013, the Riverside County Sheriff's Department arrested T.W. for burglary, receiving known stolen property, and possession of a controlled substance. On July 11, 2013, T.W. was convicted of felony possession of a controlled

substance and sentenced to 36 months of probation, 109 days of jail, and a fine.

B. INTERVIEW OF NURSE MANAGER E.J.

20. I have reviewed reports of VAMC Assistant Nurse Manager E.J.'s interview with investigators and learned the following:

a. E.J. said she had noticed that CARIAGAKAMEI had appeared to be down or depressed for the last few weeks.

b. E.J. also explained that she believed CARIAGAKAMEI could be taking VAMC medication by scanning the medication as if it was given to the patient, while actually pocketing the vials.

c. E.J. said CARIAGAKAMEI was a good employee until recently, but CARIAGAKAMEI had used another nurse's code to draw blood and entered the incorrect information, causing another RN disciplinary problems.

d. E.J. also said that CARIAGAKAMEI was good with her attendance until May 18, 2018, when she was absent without leave for two days.

C. REVIEW OF PHOTOGRAPHS TAKEN BY T.W., ALLEGEDLY WITHIN THE SUBJECT PREMISES

21. On June 13, 2018, I reviewed the six photos provided by T.W. Four of the six photographs show vials of injectable Dilaudid, three of which show a unique VAMC lot number on them (one of which is turned such that the lot number is not visible). Three of the photographs (including one of the aforementioned four) show such vials in what appears to be the

SUBJECT PREMISES, because one of the pictures shows a framed photograph in the background of a woman who appears to be CARIAGAKAMEI — I am familiar with CARIAGAKAMEI's appearance from review of her California DMV picture.

22. The photos provided by T.W. contained metadata revealing that they were taken using a Samsung Galaxy S8+ cell phone camera, and three of the six photos were taken on June 6, 2018 between 3:13PM and 3:14PM. The remaining three photos were taken on June 8, 2018 between 6:06PM and 6:07PM. Based on my training and experience, metadata on activated cell phones are regularly updated to reflect the date and time zone the device was being used in. Photographs taken on cell phones generally reflect accurate times and dates of when the photos were captured.

23. I was unable to obtain geolocation metadata from these pictures. From my discussions with other investigators, I know that T.W.'s smartphone had photograph geolocation settings turned off.

D. REVIEW OF CARIAGAKAMEI'S OMNICELL DILAUDID DOSING RECORDS REVEALS "EGREGIOUS" ANOMALIES SUGGESTIVE OF DIVERTED DOSES

24. From discussions with my colleagues, review of the records in this case, and my interview with a VAMC Clinical Pharmacist, F.B., concerning an audit-based sample of CARIAGAKAMEI's Omnicell dosing history, I am aware of the following:

a. To permit access to controlled substances by VAMC clinicians, and to secure medications, the VAMC uses a

comprehensive automated medication management machine commonly referred to as Omnicell. Most of the controlled substances kept on the VAMC's patient units are secured in this type of medication storage and distribution device.

b. Each clinician with access to Omnicell has a unique user identification and password. Most Omnicell machines allow biometrics, or a fingerprint scan, in place of a password. To retrieve controlled substances, an authorized clinician must enter his/her unique user identification and password or fingerprint into the Omnicell machine, as well as an identifier indicating which patient will be receiving the medications. Once the user enters this information, the machine allows access to the medication.

c. Omnicell records all information involving the clinician, patient, medication, type of transaction, and date and time of dispensation. The Omnicell is connected to various VA systems via Internet and allows remote access from across the country for administrative and management functions.

d. One category Omnicell records is referred to as "Waste." This refers to disposal of excess controlled substance that was not needed for administration to the patient — for example, if a vial with 2mg needs to be opened, but only 1mg is needed for a patient. To ensure control and legitimate use of controlled substances, the process of creating and monitoring "waste" requires one clinician to dispose of the medication in a waste container and another to witness such disposal, so that the waste is non-retrievable and unusable, and the remaining

portions of controlled substances do not end up in the wrong hands or impact the environment. The event always must be logged into Omnicell by both the administering clinician and an independent witness, both of whose unique user identification and passwords or fingerprints are logged. In other words, this is a highly-controlled process.

e. On June 13, 2018, F.B., a clinical pharmacist for the VAMC, reviewed Omnicell transaction logs for the past one and one-half months for morphine-based controlled substances, and based on the following, believes that CARIAGAKAMEI removed controlled substances from the VAMC:

1) On May 31, 2018, CARIAGAKAMEI removed three vials totaling 6mg from a VAMC Omnicell, administered three doses totaling 3mg, and recorded waste of 2mg, leaving 1mg unaccounted for.

2) On June 1, 2018, CARIAGAKAMEI removed one vial totaling 2mg from a VA Omnicell, and administered one dose totaling 1mg, leaving 1mg unaccounted for.

3) On June 2, 2018, CARIAGAKAMEI removed two vials totaling 4mg from a VA Omnicell, returned one vial for a total of 2mg to an Omnicell, administered one dose totaling 1mg, and recorded waste of 6mg. In other words, CARIAGAKAMEI's dispensation and waste numbers constitute a "red flag," because CARIAGAKAMEI recorded that she wasted even more than she purportedly removed from the VA Omnicell.

4) On June 3, 2018, CARIAGAKAMEI removed two vials totaling 4mg from a VA Omnicell and administered two doses

totaling 2mg, recording no waste, and thereby leaving 2mg unaccounted for.

f. In a follow-up interview on or about June 14, 2018, F.B. told me that he considered these results highly suspicious. The careful tracking of dosage, distribution, and destruction of controlled substances by the Omnicell machine and related protocols means that substances such as Dilaudid can be and are very carefully tracked, down to the mg level.

g. Specifically, F.B. characterized the results from this Omnicell sample to be "highly unusual and very suspicious," and, also, "egregious."

E. CARIAGAKAMEI LIVES AT THE SUBJECT PREMISES AND DRIVES THE SUBJECT VEHICLE

25. As described above, T.W. told investigators that CARIAGAKAMEI currently resides at the SUBJECT PREMISES and drives a car consistent with the SUBJECT VEHICLE.

26. California Department of Motor Vehicles records show that the SUBJECT VEHICLE is registered to CARIAGAKAMEI, but at an address other than the SUBJECT PREMISES.

27. On or about June 14, 2018, VA-OIG agents conducted surveillance at the SUBJECT PREMISES, and saw CARIAGAKAMEI leave the SUBJECT PREMISES with a dog and depart in the SUBJECT VEHICLE.

F. SUBJECT LOCKER IS USED BY CARIAGAKAMEI

28. From discussions with my colleagues and review of reports of this investigation, and my own work on this investigation I know the following:

a. On or about June 13, 2018, I received a photograph of the SUBJECT LOCKER, which has CARIAGAKAMEI's name taped on it.

b. On June 14, 2018, a supervisor at the VAMC confirmed that the SUBJECT LOCKER is used by CARIAGAKAMEI.

G. CURES DATABASE CAN REVEAL DOCTOR-SHOPPING

29. From discussions with my colleagues and review of reports of this investigation, and my own work on this investigation I know the following:

a. The CURES program provides oversight and records of Schedule II, III, and IV controlled substances prescriptions dispensed in California. Therefore, California medical personnel dispensing controlled substances and patients obtaining controlled substances will have records in CURES pertaining to their transaction history. CURES data are unique for each person, relying on and tracking patients' personally identifying information, which they must provide before receiving controlled substances pursuant to a prescription.

b. Clinicians who divert drugs from the VA frequently obtain controlled substances from multiple physicians, commonly known as "doctor shopping," which itself may constitute a violation of the prohibition in 21 U.S.C. § 843 (a)(3) against obtaining a controlled substance by "deception."

c. Thus, if CARIAGAKAMEI were "doctor-shopping," i.e., attempting to fill prescriptions at various pharmacies pursuant to prescriptions from various doctors, CURES data could reflect such efforts.

H. REQUEST FOR VISUAL INSPECTION OF CARIAGAKAMEI'S PERSON

30. As stated in greater detail in Attachment A-5 and in Attachment B, the warrant I am applying for would permit a visual inspection of CARIAGAKAMEI's bare hands, arms, and feet. Based on my training and experience and on my conversation with more experienced agents, I understand that a visual inspection of a suspected drug user's hands, arms, and feet can provide evidence of drug use or absence of drug use, which would be evidence of one or more of the SUBJECT OFFENSES. Specifically, as stated in greater detail in Attachment B, I am requesting authorization to conduct a visual inspection of CARIAGAKAMEI's bare hands, arms, and feet for such evidence, including needle ("track") marks on her body. I am not seeking at this time any more intrusive of a search than for her hands, arms, and feet.

I. TRAINING AND EXPERIENCE CONCERNING CONTROLLED SUBSTANCE DIVERSION OFFENSES

31. Based on my training, experience, and discussions with other law enforcement officers, I know the following:

a. Medical personnel intending to divert controlled substances typically use workplace storage areas, such as their hospital lockers to store securely controlled substances that they have taken off the hospital floor.

b. Such persons also typically place diverted controlled substances in their cars at the end of their shifts, so that they may transport the controlled substances away from the treatment centers for their own personal use or subsequent

distribution, or so that they may use or distribute the diverted controlled substances in or from their cars.

c. Drug diverters who are diverting IV-administered controlled substances for personal use will frequently use needles, which leave track marks on various locations on their body.

V. TRAINING AND EXPERIENCE REGARDING THE USE OF DIGITAL DEVICES IN DRUG OFFENSES

32. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Those who distribute drugs to others often maintain books, receipts, notes, ledgers, bank records, and other records relating to the sale and distribution of illegal drugs. The aforementioned records are often maintained where the drug distributor has ready access to them, such as on their cell phones and other digital devices.

b. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion of whether or not participants will bring weapons to a deal. In addition, it is common for people engaged in drug distribution to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these

photos to each other and others to boast about the drugs or facilitate drug sales.

c. Drug distributors often keep the names, addresses, and telephone numbers of associates in their cars and on their digital devices. Drug distributors also often keep records of meetings with associates, customers, and suppliers on their digital devices, including in the form of calendar entries and location data.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES GENERALLY

33. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of

digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it takes time to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the type of digital device, operating system, and software application being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or

more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.¹ Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary

¹ These statements do not generally apply to data stored in volatile memory such as random-access memory, or "RAM," which data is, generally speaking, deleted once a device is turned off.

directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that

show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a

controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

34. As discussed herein, based on my training and experience I believe that digital devices will be found during the search.

a. I know from my training and experience and my review of publicly available materials that several hardware and software manufacturers offer their users the ability to unlock their devices through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint-recognition, face-recognition, iris-recognition, and retina-recognition. Some devices offer a combination of these biometric features and enable the users of such devices to select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple Inc. ("Apple") offers a feature on some of its phones and laptops called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which on a cell phone is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the phone, and on a laptop is located on the right side of the "Touch Bar" located directly above the keyboard. Fingerprint-recognition features are increasingly common on modern digital devices. For example, for Apple products, all iPhone 5S to

iPhone 8 models, as well as iPads (5th generation or later), iPad Pro, iPad Air 2, and iPad mini 3 or later, and MacBook Pro laptops with the Touch Bar are all equipped with Touch ID. Motorola, HTC, LG, and Samsung, among other companies, also produce phones with fingerprint sensors to enable biometric unlock by fingerprint. The fingerprint sensors for these companies have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. To activate the facial-recognition feature, a user must hold the device in front of his or her face. The device's camera analyzes and records data based on the user's facial characteristics. The device is then automatically unlocked if the camera detects a face with characteristics that match those of the registered face. No physical contact by the user with the digital device is necessary for the unlock, but eye contact with the camera is often essential to the proper functioning of these facial-recognition features; thus, a user must have his or her eyes open during the biometric scan (unless the user previously disabled this requirement). Several companies produce digital devices equipped with a facial-recognition-unlock feature, and all work in a similar manner with different degrees of sophistication, e.g., Samsung's Galaxy S8 (released Spring 2017) and Note8 (released Fall 2017), Apple's iPhone X (released Fall 2017). Apple calls its facial-recognition unlock feature "Face

ID." The scan and unlock process for Face ID is almost instantaneous, occurring in approximately one second.

d. While not as prolific on digital devices as fingerprint- and facial-recognition features, both iris- and retina-scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that are unique and stable. Iris-recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data from the person's eyes. The device is then unlocked if the camera detects the registered eye. Both the Samsung Galaxy S8 and Note 8 (discussed above) have iris-recognition features. In addition, Microsoft has a product called "Windows Hello" that provides users with a suite of biometric features including fingerprint-, facial-, and iris-unlock features. Windows Hello has both a software and hardware component, and multiple companies manufacture compatible hardware, e.g., attachable infrared cameras or fingerprint sensors, to enable the Windows Hello features on older devices.

35. In my training and experience, users of electronic devices often enable the aforementioned biometric features

because they are considered to be a more convenient way to unlock a device than entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

36. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features have been enabled. This can occur when a device has been restarted or inactive, or has not been unlocked for a certain period of time. For example, with Apple's biometric unlock features, these circumstances include when: (1) more than 48 hours has passed since the last time the device was unlocked; (2) the device has not been unlocked via Touch ID or Face ID in eight hours and the passcode or password has not been entered in the last six days; (3) the device has been turned off or restarted; (4) the device has received a remote lock command; (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made; or (6) the user has activated "SOS" mode by rapidly clicking the right side button five times or pressing and holding both the side button and either volume button. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time. I do not

know the passcodes of the devices likely to be found during the search.

37. In my training and experience, the person who is in possession of a device or has the device among his or her belongings, or in his or her home or car at the time the device is found is likely a user of the device.

a. For these reasons, if while executing the warrant, the warrant I am applying for would permit law enforcement personnel to, with respect to biometrically enabled devices that fall within the scope of the warrant: (1) compel the use of the CARIAGAKAMEI's thumb- and/or fingerprints on the device(s); and (2) hold the device(s) in front CARIAGAKAMEI's face with her eyes open to activate the facial-, iris-, and/or retina-recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

38. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. CONCLUSION

39. Based on the foregoing, I believe there is probable cause to believe that evidence, fruits, and instrumentalities of

the SUBJECT OFFENSES, as described in Attachment B to this Affidavit, will be found within the locations described in Attachments A-1 through A-5.

CHRIST KONG
Special Agent
Office of Inspector General
Department of Veterans Affairs

Subscribed to and sworn before
me this ____ day of June, 2018.

UNITED STATES MAGISTRATE JUDGE